Newsletter

ANNO 2024	n. 05/ 2024	maggio 2024

Le criticità dei porti e delle infrastrutture portuali

I porti sono da sempre al centro delle politiche di sviluppo di ogni paese. Essi hanno un ruolo fondamentale per gli interessi militari, commerciali, sociali e politici di uno Stato, sono parte integrante del sistema infrastrutturale di una nazione e per tale motivo annoverati tra le infrastrutture critiche.
In ambito nucleare, si definisce criticità lo stato di un reattore nel quale si innesca la reazione a catena delle fissioni. Se volessimo utilizzare tale circonlocuzione, potremmo definire la criticità in ambito portuale quell'insieme di attività principali e complementari che intercorrono tra la nave, le facilities portuali e le infrastrutture retroportuali, la cui interruzione implica la riduzione o la sospensione degli approvvigionamenti.

Prima di approfondire le criticità legate alle operazioni portuali in ambito commerciale, risulta essenziale introdurre e definire i principali attori del trasporto marittimo, ovvero la nave e il porto.
La nave è un mezzo di trasporto con elevata capacità di carico che utilizza le vie d'acqua fluviali e marittime per lo spostamento di merci e persone. Le navi si possono distinguere in: navi passeggeri – che possono ospitare più di cinquemila persone tra membri d'equipaggio e passeggeri – e navi mercantili che trasportano diverse tipologie di merci (carichi secchi e liquidi). Esse sono soggette a normative internazionali che ne stabiliscono i criteri minimi di progettazione, costruzione (certificati da enti di classifica, autorizzati dalle amministrazioni di bandiera) ed equipaggiamento, al fine di salvaguardare la vita umana in mare e l'ambiente.
Oltre ai requisiti in termini di safety, le navi - come i porti - sono sottoposte a norme e regolamenti sulla security. Dopo gli attentati dell'11 settembre 2001 e l'espandersi della minaccia terroristica a livello globale, nel 2002 l'IMO (International Maritime Organization), ha pubblicato l'ISPS code (International Ship and Port Facility Security Code). Il codice prevede norme internazionali e procedure di security da applicare alle navi commerciali e alle facilities portuali. Inoltre, con lo sviluppo delle tecnologie digitali in ambito navale e l'implementazione delle cybertechnologies, divenute oramai essenziali per le operazioni di bordo, l'IMO ha introdotto delle linee guida sulla cybersecurity, denominate maritime cyber risk management (MSC – FAL.1/Circ.3/Rev.2 – 7 June 2022)[1].
Il porto è lo spazio di mare dove le navi possono sostare con sicurezza al riparo dalle onde e dalle correnti, compiere le operazioni di sbarco e d'imbarco di passeggeri e merci, rifornimenti e riparazioni. Ogni porto possiede delle caratteristiche geografiche, morfologiche e infrastrutturali che ne definiscono specificità e particolarità. A differenza del passato, oggi i porti includono una serie di servizi funzionali alle realtà industriali di privati del luogo ivi collocate e terminalisti titolari di concessioni demaniali (terminal container, petroliferi, LNG e depositi) che svolgono attività d'interesse pubblico interne agli stessi e collegati alla filiera logistica retroportuale.
Pertanto, i porti sono veri e propri nodi del trasporto intermodale inseriti in corridoi commerciali collegati con l'Europa e il resto del mondo (TEN-T corridor, Adriatic port corridor system,

[1] https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx

Mediterranean corridor, Helsinki corridor, ecc.)[2]. Quest'ultimo aspetto è centrale per le politiche governative di sviluppo economico e di posizionamento geopolitico.

Tutte le attività portuali legate al transhipment delle merci o al transito dei passeggeri sono attività critiche. Il "mimetismo" e "l'invisibilità" del transito di grandi volumi di merci e passeggeri sono ben note alle organizzazioni criminali che sovente le utilizzano per il contrabbando internazionale di sostanze stupefacenti, traffico illegale di armi e di esseri umani. L'ultimo rapporto dell'Europol, *Serious and organized crime threat assessment*[3], ha evidenziato l'elevata specificità e importanza del trasporto marittimo per la conquista di nuovi mercati da parte del crimine transnazionale.
Nondimeno sono i rischi provenienti dagli attacchi cibernetici. I software multifunzione interconnessi alle navi e ai terminal, velocizzano e semplificano le operazioni portuali, rendendole però vulnerabili dal punto di vista cibernetico. Un esempio sono i software utilizzati per le operazioni di carico e scarico dei container dalle navi. Il posizionamento e la movimentazione dei container sono gestiti direttamente dal terminal portuale attraverso l'impiego di reti intranet in comunicazione con la nave che monitora le operazioni per la verifica della stabilità e assetto. Recentemente il Congresso degli Stati Uniti ha disposto indagini approfondite sulle gru di fabbricazione cinese utilizzate nei terminal container, dopo che le autorità hanno rinvenuto dispositivi e attrezzature per le telecomunicazioni da remoto, non appartenenti alle componenti di funzionamento. La scoperta dei dispositivi installati sulle gru è stata definita pericolosa per la sicurezza nazionale, dei porti e delle infrastrutture.
Un altro esempio di operazioni portuali critiche sono quelle relative al transhipment di gas naturale liquefatto. Un terminal LNG riceve il gas liquefatto dalle navi, trasformandolo in forma gassosa mediante gli impianti di rigassificazione. Tali processi sono eseguiti con l'ausilio di tecnologie che presentano vulnerabilità fisiche e cibernetiche. Il rapporto emesso dall'US Department of Commerce nel 2023, denominato *Cybersecurity framework profile for Liquefied Natural Gas*[4], pone in evidenza tutti i rischi derivanti dalle operazioni di transhipment e sottolinea l'importanza del fattore umano quale elemento complementare allo studio dei rischi cyber.

In conclusione, in un paese come l'Italia, caratterizzato da più di ottomila chilometri di coste e dotato di trecentocinquantuno porti, dei quali cinquantotto di rilievo nazionale[5], è fondamentale sostenere investimenti pubblici e privati mirati alla ricerca scientifica e all'innovazione tecnologica applicata alle operazioni portuali e alla filiera logistica. Lo sviluppo delle competenze in termini di safety e security degli enti pubblici e privati (i primi, interessati alla gestione e controllo dei porti, i secondi alla loro operatività) è imprescindibile e decisivo nell'attuazione di programmi strategici volti alla competizione commerciale globale.

Sante Grande

Comandante di marina mercantile e consulente marittimo libero professionista, ha studiato presso l'Accademia Italiana della Marina Mercantile ed è laureato in Scienze Politiche e delle Relazioni Internazionali. Attualmente frequenta il Master in Diritto Marittimo, Portuale e della Logistica presso l'Università di Bologna. E' socio AIIC.

[2] https://transport.ec.europa.eu/transport-themes/infrastructure-and-investment/trans-european-transport-network-ten-t_en
[3] https://www.europol.europa.eu/publications-events/main-reports/socta-report
[4] https://www.nist.gov/publications/cybersecurity-framework-profile-liquefied-natural-gas
[5] https://dati.mit.gov.it/catalog/dataset/porti/resource/661bba97-829e-453e-8923-97023de9fced

ATTIVITA' DELL'ASSOCIAZIONE

RINNOVO ASSOCIATIVO ANNO 2024

Il 31 dicembre 2023 è scaduto il periodo associativo. Invitiamo pertanto i signori soci a rinnovare con sollecitudine l'iscrizione alla nostra associazione versando il relativo contributo.
La quota per il rinnovo individuale è di euro 50 e può essere versata con bonifico sul conto corrente presso Banca Intesa Business, IBAN IT17B0306909606100000114955, intestato a AIIC Associazione Italiana esperti in Infrastrutture Critiche, indicando come causale "rinnovo socio ordinario nome e cognome anno 2024".
Le quote e le modalità di rinnovo per i soci collettivi sono contenute nel sito AIIC www.infrastrutturecritiche.it.
Ricordiamo che **la data limite per il rinnovo annuale, come da regolamento, è fissata al 31 marzo 2024. Dopo questa data, si decade dalla qualifica di socio e sarà necessario procedere ad una nuova iscrizione versando anche il contributo per le spese di segreteria.**
La nostra segreteria è a disposizione, per informazioni, alla mail segreteria@infrastrutturecritiche.it.

PUBBLICAZIONE DI ARTICOLI DA PARTE DI SOCI E PARTECIPAZIONE AD EVENTI

Ricordiamo ai soci che nella pubblicazione di un articolo o di un libro **non è possibile** firmarsi qualificandosi come "Associazione Italiana esperti in Infrastrutture Critiche", in quanto solo chi ha la rappresentanza legale dell'Associazione può esprimersi a nome AIIC.
La stessa regola vale anche se si partecipa ad un evento in qualità di organizzatore, relatore o chairman.

La possibilità di pubblicare o partecipare ad eventi a nome AIIC deve essere approvata dal Consiglio Direttivo dell'Associazione su richiesta del socio che, pertanto, è pregato di contattare il CD con ragionevole anticipo.

È invece raccomandato indicare, nel proprio profilo professionale, l'appartenenza ad AIIC, Associazione Italiana esperti in Infrastrutture Critiche, in qualità di socio.

NUOVO SITO WEB AIIC – FONTE UFFICIALE DELL'ASSOCIAZIONE

Ricordiamo che è attivo il nuovo sito dell'Associazione Italiana Esperti in Infrastrutture Critiche.
L'indirizzo è sempre **www.infrastrutturecritiche.it** ma il sito è stato completamente rinnovato, sia nelle veste grafica che nei contenuti e nelle funzioni a disposizione.
Vi invitiamo a consultarlo e anche a farci pervenire le vostre osservazioni: i vostri suggerimenti sono sempre preziosi e ci aiutano a migliorare il prodotto.

Vi ricordiamo inoltre che il sito web www.infrastrutturecritiche.it rappresenta la **fonte ufficiale dell'associazione**, accessibile a tutti, e contiene tutte le informazioni necessarie per un corretto svolgimento della vita associativa.
Potete scriverci al nostro solito indirizzo email: *segreteria@infrastrutturecritiche.it*

ASSEMBLEA GENERALE DEI SOCI AIIC

In data 17 aprile 2024 si è svolta via web la riunione del Consiglio Direttivo di AIIC, avente come oggetto la convocazione dell'assemblea generale dei soci per l'approvazione del bilancio consuntivo 2023 e preventivo 2024.
Dopo attenta valutazione il C.D. ha deciso di convocare, in modalità online, l'Assemblea Generale dei Soci per l'approvazione del bilancio il giorno di mercoledì 15 maggio 2024 alle ore 24 in prima convocazione e per il giorno **martedì 21 maggio 2024 alle ore 17.00**, in seconda convocazione.
Sarà cura del Consiglio Direttivo comunicare ai soci entro il 16 maggio 2024 le modalità di collegamento.

NUOVO GRUPPO DI LAVORO AIIC
Critical Infrastructures Resilience and Artificial Intelligence
(Resilienza delle Infrastrutture Critiche e Intelligenza Artificiale)

INVITO A PARTECIPARE

Il Consiglio Direttivo AIIC nella sua riunione del 17 Aprile 2024 ha approvato la nascita del GdL "Critical Infrastructures Resilience and Artificial Intelligence" (Resilienza delle Infrastrutture Critiche e Intelligenza Artificiale).
Tutti i Soci AIIC che intendano partecipare sono invitati a manifestare la loro disponibilità entro il 24 Maggio 2024, inviando una mail al Coordinatore s.bologna@infrastrutturecritiche.it e per conoscenza alla Segreteria segreteria@infrastrutturecritiche.it Di seguito i dati salienti del GdL proposto.

Coordinatore: Sandro Bologna
Data inizio lavori: 01.06.2024
Durata max: 12 mesi
Lingua di redazione: inglese
Riferimenti: tutti i Documenti a cui si fa riferimento sono disponibili nella Homepage del sito AIIC

DESCRIZIONE DEL GdL E LISTA DEGLI ARGOMENTI TRATTATI

Tutte le informazioni di dettaglio e un indice degli argomenti da trattare sono presenti nella Homepage del sito AIIC. Questo indice fornisce un quadro completo per esplorare le interconnessione tra resilienza, infrastrutture critiche e intelligenza artificiale, che coprono vari aspetti come la comprensione della resilienza, le applicazioni di intelligenza artificiale, i casi di studio, la valutazione

dei rischi, le considerazioni politiche, le innovazioni tecnologiche, l'etica, le implicazioni e direzioni future.

Vista l'attualità dell'argomento, invitiamo caldamente i Soci a partecipare!

Si ricorda che la partecipazione ai Gruppi di Lavoro AIIC è riservata ai Soci AIIC in regola con i pagamenti associativi.

WEBINAR AIIC

La Direttiva (UE) 2022/2557 sulla resilienza dei soggetti critici (Critical Entities Resilience)

mercoledì 12 giugno 2024 ore 15.00-17.00

La nuova direttiva CER completa il panorama normativo europeo sulle infrastrutture critiche, riconciliando, in un mutato quadro geopolitico, la sicurezza negli ambiti cibernetico e cinetico, in una prospettiva all-hazard e risk-based, prevedendo norme armonizzate volte a garantire la fornitura di servizi essenziali nel mercato interno, a migliorare la resilienza degli operatori pubblici e privati, ora definiti soggetti critici, e la cooperazione transfrontaliera tra le autorità competenti, mutuando, di massima, il quadro regolatorio già adottato per il settore dei trasporti, in particolare nell'ambito dell'aviazione civile.

Il webinar sarà tenuto da Alberto Caruso de Carolis.

Ufficiale superiore in congedo della Guardia di Finanza ove ha svolto incarichi addestrativi, investigativi, informativi e di collaborazione internazionale, dal 2002, è stato dirigente presso una società di gestione aeroportuale in incarichi di staff nell'alta direzione, aviation security, internal audit e Rapporti con la Pubblica Amministrazione, e presso Assaeroporti, coordinatore del gruppo di lavoro "Rapporti con la PA, Privacy e informatica", poi divenuto "Cybersecurity". Attualmente partner in società di consulenza per l'area Corporate Governance, Safety per rischio sociale, rapporti con la Pubblica Amministrazione, e sviluppo progetti nel settore law enforcement e difesa. Docente presso il Master di primo livello "Crisis & Disaster Management" dell''Università Cattolica del Sacro Cuore di Milano, coautore nel libro "Guerra economica - Modelli decisionali e intelligence economico finanziaria", e recentemente nella pubblicazione di AIIC "La protezione degli spazi pubblici".

La partecipazione è aperta ai soci e ai simpatizzanti di AIIC, previa iscrizione inviando una mail a:
segreteria@infrastrutturecritiche.it
A coloro che si iscriveranno entro la data del 5 giugno 2024 verrà inviata una mail di conferma con i dati relativi al collegamento.

VISITA GRATUITA ALLA MOSTRA CYBSEC-EXPO 2024

AIIC ha concesso il patrocinio alla mostra CYBSEC-EXPO 2024, che si svolgerà a Piacenza nei giorni 29-31 maggio 2024.
Maggiori informazioni sull'evento, expo e conference, che riguarda la Cybersecurity, la protezione dei dati e delle infrastrutture critiche, possono essere consultate al seguente link: https://cybsec-expo.it

Con l'occasione, i soci AIIC possono visitare gratuitamente la mostra piacentina partecipando ai numerosi convegni che si terranno durante i 3 giorni di apertura.
Per ottenere il biglietto invito in formato elettronico personalizzato si può scrivere alla segreteria AIIC segreteria@infrastrutturecritiche.it

NEWS E AVVENIMENTI

Programmi a sostegno della trasformazione digitale e verde del sistema energetico - I programmi dell'UE a sostegno della ricerca e dell'innovazione, della diffusione e dell'infrastruttura di connettività transfrontaliera sono fondamentali per la digitalizzazione del sistema energetico.
Promuovere la ricerca e l'innovazione nell'ambito di Orizzonte 2020 e Orizzonte Europa
L'impegno dell'UE a sostenere la ricerca e l'innovazione (R&I) nel settore energetico è evidente nelle notevoli dotazioni di finanziamento concesse nell'ambito di Orizzonte 2020 e Orizzonte Europa. Orizzonte 2020, lanciato nel 2015, ha stanziato circa 1 miliardo di EUR a progetti di R&I incentrati sulle reti intelligenti, lo stoccaggio dell'energia, le isole energetiche e la digitalizzazione dell'energia. L'iniziativa BRIDGE riunisce molti di questi progetti di ricerca e innovazione per consentire la condivisione delle conoscenze, promuovere l'innovazione e promuovere l'uso di tecnologie all'avanguardia per accelerare la trasformazione verde e digitale del sistema energetico.

Progetti come InterConnect , che ha ricevuto quasi 30 milioni di euro di finanziamenti dell'UE, stanno lavorando a soluzioni avanzate per collegare e convergere case ed edifici digitali con il sistema elettrico. Open DEI supporta le piattaforme digitali di prossima generazione nella produzione, nell'agricoltura, nell'energia e nell'assistenza sanitaria promuovendo l'innovazione, la collaborazione, la sperimentazione su larga scala e gli sforzi di standardizzazione e per consentire una piattaforma di dati industriale più unificata *(continua)*.
https://www.puntosicuro.it/digitalizzazione-C-147/programmi-a-sostegno-della-trasformazione-digitale-verde-del-sistema-energetico-AR-24130
PuntoSicuro *- Redazione- 19/03/2024*

Clima e diritti umani: CEDU, Stati obbligati a proteggere cittadini
Per la 1° volta viene riconosciuto l'obbligo di tutelare clima e diritti umani
La Svizzera ha violato i diritti umani dei suoi cittadini perché non ha fatto abbastanza per tagliare le emissioni di gas serra. Lo ha stabilito la Corte europea dei diritti dell'uomo (ECHR, CEDU in italiano) dopo un anno di lavori nella sentenza, emessa il 9 aprile, sul contenzioso climatico avanzato nel 2016 da KlimaSeniorinnen Schweiz, un gruppo di 2mila anziane svizzere con un'età media di 73 anni. La sentenza ha una portata storica e riscrive il rapporto tra clima e diritti umani: la decisione dell'ECHR è legalmente vincolante, influenzerà altri tribunali e darà più chances ai contenziosi climatici in corso e futuri. È la prima volta che un tribunale internazionale stabilisce che la crisi climatica danneggia i diritti umani. *(continua…)*
https://www.rinnovabili.it/mercato/politiche-e-normativa/clima-e-diritti-umani-cedu/
Rinnovabili.it *– Lorenzo Marinone•10 Aprile 2024*

Centrali idroelettriche: l'incidente alla centrale di Bargi e la sicurezza - L'esplosione nella centrale idroelettrica di Bargi sul bacino artificiale di Suviana: le prime informazioni sulla dinamica dell'incidente, le reazioni, i dati e il funzionamento delle centrali idroelettriche.
Non c'è dubbio che, come accade generalmente nei grandi incidenti di lavoro, per fare delle serie ipotesi sulle cause, sulle concause, sulle criticità che hanno portato all' esplosione nella centrale idroelettrica di Bargi sul bacino artificiale di Suviana, nell'Appennino Bolognese, dovrà ancora passare del tempo.
Come abbiamo raccontato ieri nell'articolo " L'esplosione nella centrale idroelettrica del bacino di Suviana" le indagini potranno procedere solo dopo che saranno conclusi i lavori dei soccorritori e quando sarà possibile accedere ai luoghi in cui è avvenuta l'esplosione.
Ricordiamo brevemente quello che è possibile conoscere, per il momento, riguardo alla dinamica dell'incidente.
Secondo quanto ricostruito dai Vigili del Fuoco intorno alle 14.30 è avvenuta una violenta esplosione all'ottavo piano ribassato della struttura (la struttura scende sottoterra per 60 metri), mentre al nono piano è avvenuta un'inondazione dovuta a un tubo di raffreddamento della turbina.
Sembrerebbe che ieri era in corso una prova di messa in esercizio, che precede il collaudo ufficiale, che avrebbe concluso alcuni lavori di manutenzione straordinaria appaltati a varie aziende. In questa fase sarebbe avvenuta l' esplosione.
Al di là delle prime riflessioni su quanto avvenuto, ad esempio riguardo alle difficoltà iniziali nel conoscere con precisione numero e nomi dei lavoratori presenti nella centrale, cerchiamo di raccogliere le reazioni alla notizia dell'incidente e ulteriori informazioni attraverso i documenti pubblicati in questi ultimi anni sulla sicurezza nelle centrali idroelettriche. *(continua…)*
https://www.puntosicuro.it/infortuni-sul-lavoro-C-138/centrali-idroelettriche-l-incidente-alla-centrale-di-bargi-la-sicurezza-AR-24236/

PuntoSicuro *– Redazione – 11 aprile 2024*

Russia-linked APT28 group used a previously unknown tool, dubbed GooseEgg, to exploit Windows Print Spooler service flaw.

Microsoft reported that the Russia-linked APT28 group (aka "Forest Blizzard", "Fancybear" or "Strontium" used a previously unknown tool, dubbed GooseEgg, to exploit the Windows Print Spooler flaw CVE-2022-38028.

Since at least June 2020, and possibly earlier, the cyberespionage group has used the tool GooseEgg to exploit the CVE-2022-38028 vulnerability. This tool modifies a JavaScript constraints file and executes it with SYSTEM-level permissions. Microsoft has observed APT28 using GooseEgg in post-compromise activities against various targets, including government, non-governmental, education, and transportation sector organizations in Ukraine, Western Europe, and North America.

While GooseEgg is a simple launcher application, threat actors can use it to execute other applications specified at the command line with elevated permissions. In a post-exploitation scenario, attackers can use the tool to carry out a broad range of malicious activities such as remote code execution, installing backdoors, and moving laterally through compromised networks. (continua…)

https://securityaffairs.com/162154/apt/apt28-gooseegg-tool-win-bug.html

SecurityAffairs *- Pierluigi Paganini - April 22, 2024*

2023: A 'Good' Year for OT Cyberattacks

Attacks increased by "only" 19% last year. But that number is expected to grow significently.

COMMENTARY

Waterfall Security Solutions, in collaboration with ICS Strive, recently released its "2024 Threat Report." The bad news is that, in 2023, there were 68 cyberattacks that took down more than 500 physical operations. The good news (sort of) is that this is only 19% more attacks than the previous year. What's going on? Ransomware attacks with physical consequences are down slightly, hacktivist attacks are constant, and everything else is increasing. The report's authors conclude that the 19% increase is most likely an aberration, and that we'll see an increase closer to 90% to 100% in 2024.

The Details

Waterfall's operational technology (OT) security threat report is the most cautious in the industry — it tracks only deliberate cyberattacks that caused physical consequences in building automation, heavy industry, manufacturing, and critical industrial infrastructures *in the public record*. That is, no private or confidential disclosures. The complete data set for the report is included in its appendix. This means the report is certain to be an underestimate of what's really happening in the world, because the authors report regular confidential disclosures that they cannot include in their counts.

OT incidents since 2010. Source: "2024 Threat Report," Waterfall Security Solutions, in collaboration with ICS Strive

More Attacks

In spite of this underestimate, cyberattacks that met the inclusion criteria continue to increase, nearly doubling annually since 2019. This is a big change from 2010–2019, when OT attacks with physical consequences were flat, bouncing around between zero and five attacks annually. (continua…)

https://www.darkreading.com/endpoint-security/2023-good-year-for-ot-cyberattacks

Darkreading *-Andrew Ginter, - April 24, 2024*

Città resilienti, ecco il piano per New York - Dopo i disastri prodotti dagli uragani Sandy (2012) e Ida (2021) l'obiettivo è rendere la Grande Mela una città a prova di pioggia. L'esperienza di Rebuild by Design e la ricerca condotta dallo studio internazionale One Architecture & Urbanism. Ecco le soluzioni tecniche per gestire le acque piovane in occasione di eventi estremi.
29 ottobre 2012. L'uragano Sandy si abbatte sulla costa orientale degli Stati Uniti e a New York strade, tunnel, metropolitane, seminterrati vengono inondati dall'acqua lasciando la città al buio e facendo danni per oltre 63 miliardi di dollari. Un evento che lasciò il segno, in particolare nel cuore di Manhattan. Fu da quel dramma che la Grande Mela iniziò ad affrontare gli effetti indotti dai cambiamenti climatici .
Nasce Rebuild by Design *(continua).*
https://www.ingenio-web.it/articoli/citta-resilienti-ecco-il-piano-per-new-york/
INGENIO - *Pietro Mezzi – 29 aprile2024*

Supply chain e sicurezza dei dati: come evitare l'effetto domino
Quando si parla di protezione dei dati, quello tra aziende e catena di fornitura è un equilibrio che va costantemente monitorato e protetto: un singolo punto debole può infatti innescare una reazione a catena, sull'intera struttura. Il recente caso Synlab e il precedente di Westpole sono esemplari per capire l'importanza di una corretta gestione della supply chain
La **compromissione** di **un anello della catena di gestione dei dati** è un evento che coinvolge tutti gli attori che la compongono: un problema di sicurezza che si verifica presso un provider di servizi utilizzato da diversi clienti può infatti scatenare una catena di eventi simile a un "**effetto domino**", con ripercussioni su ciascun cliente coinvolto.
Di conseguenza, **le misure di sicurezza lungo la catena di fornitura** non sono solo importanti, ma vitali e il ruolo del **titolare del trattamento** dei dati assume una rilevanza centrale.
Indice degli argomenti

Corretta gestione della catena dei fornitori: i casi Synlab e Westpole
Ci insegnano molto, in questo senso, i casi Synlab di questi giorni e quello Westpole di dicembre scorso, per capire **l'importanza di una corretta gestione della catena dei fornitori** e del notevole impatto di un possibile incidente di sicurezza.
Il cyberattacco a Synlab e le ripercussioni
Synlab è uno dei principali fornitori di servizi di diagnosi medica, i cui centri italiani di diagnostica medica, anche relativi a dati genetici, sono distribuiti in nove Regioni italiane. Si è vista costretta a **sospendere a livello nazionale tutte le attività presso i punti prelievo** (prelievi e consegna campioni), incluso il download e il ritiro dei referti dai propri clienti.Tale blocco di attività, in considerazione della particolarità e diffusività dei servizi svolti, anche su mandato di aziende sanitarie

pubbliche, ha provocato **l'impossibilità di accedere ai dati sanitari di un enorme numero di cittadini** e potrebbe provocare persino la perdita di una serie di loro campioni biologici, materiali altamente deperibili e le cui preziose informazioni rimangono stabili soltanto per brevi periodi.Nell'ultimo **aggiornamento** sul sito Synlab, del 28 aprile, l'azienda fa sapere che "prosegue il lavoro per ripristinare l'attività a seguito dell'attacco cybercriminale".(continua…)
https://www.agendadigitale.eu/sicurezza/supply-chain-e-sicurezza-dei-dati-come-evitare-leffetto-domino/
Agendadigitale- *Filomena Polito, Michele Principi - 29 apr 2024*

IA generativa: rivoluzione o bolla? Ecco le tendenze per decifrarne il futuro
L'IA generativa, specie dopo il lancio di ChatGPT, sta generando notevoli aspettative, con un aumento di valore per le aziende coinvolte nel tech stack. Ma le implicazioni economiche sono incerte. Sfide come investimenti, privacy, e impatto ambientale emergono, mentre regolamentazione e geopolitica influenzano il suo futuro
L'**intelligenza artificiale** (AI-Artificiale Intelligence) non è nata certo con **ChatGPT**. È un fatto noto, ma credo opportuno ricordarlo, che l'idea di AI nasce insieme con i primi calcolatori e che il test di Turing di cui spesso si parla, che "misura" l'intelligenza di un modello di AI a raffronto con l'umana, è stato presentato per la prima volta in un **articolo del 1950** ("Computing machinery and intelligence").
Indice degli argomenti

IA generativa: una "nuova" Internet o un "nuovo" metaverso?
Il suo sviluppo progressivo – parallelo e profondamente influenzato dall'evoluzione della capacità e velocità di calcolo – ha portato alla messa a punto di **applicazioni nei comparti più diversi**, molte delle quali diventate ai nostri occhi così usuali da perdere la qualifica di intelligenti. E tuttora i confini dell'AI si mantengono più ampi di quelli della sua componente generativa.
Che cosa ha di particolare allora l'AI generativa, al cui lancio da parte di OpenAI il 22 ottobre 2022 ha fatto seguito una grandiosa campagna mediatica – orchestrata in primo luogo da Microsoft (principale finanziatore e attuale azionista di maggioranza di OpenAI) – che ha contribuito alla **crescita di grandissime aspettative** sull'impatto che essa potrà avere sull'economia e sulla società in generale, nonché più specificamente

- **sulle imprese che utilizzeranno i suoi modelli per rendere più efficiente la loro macchina organizzativa** e/o per mettere a punto nuovi prodotti, servizi o modelli di business,
- **sulle imprese che ne svilupperanno modelli nuovi e sempre più potenti** e/o che, con le loro infrastrutture e i loro servizi, abiliteranno l'accesso ai modelli stessi delle imprese utilizzatrici e degli altri attori dell'economia e della società?

In estrema sintesi, proprio per come è concepita, mi piace definirla come **una tecnologia che "ha una grande fame" di soldi, dati ed energia elettrica** e che vorrebbe essere circondata – dati i temi di cui si occupa (mettere a punto intelligenze che potrebbero superare quella umana o addirittura provocare la fine stessa della razza umana) – da un rispetto quasi religioso.
Passando alla domanda che appare nel titolo di questo paragrafo – una "nuova" Internet o un "nuovo" metaverso? – non farò scommesse, ma cercherò di **fornire una serie di elementi che aiutino a capire a che punto siamo e quali siano le maggiori difficoltà da superare.**

Il tech stack

Ho diviso nel punto precedente, anche se la linea di separazione non è così netta, le imprese potenziali utilizzatrici dell'AI generativa da quelle che **sviluppano i nuovi modelli e/o che, con le loro infrastrutture e i loro servizi**, abilitano l'accesso ai modelli stessi delle imprese utilizzatrici e degli altri attori dell'economia e della società. Per denotare l'insieme di queste imprese viene spesso utilizzato il termine tech stack. È evidente – per una tecnologia articolata e complessa come l'AI generativa – come sia compito delle imprese del *tech stack* fare gli investimenti necessari per far decollare il tutto, e allo stesso tempo come esse siano le prime a

- essere oggetto dell'attenzione del mercato finanziario, per i vantaggi di cui godranno se l'Ai generativa avrà successo, e viceversa,
- vedere apparire nei propri bilanci sia i ricavi derivanti dalle prime vendite sia (all'inizio molto più rilevanti) i costi – correnti e in conto capitale – che dovranno sopportare.

Mentre solo più tardi si potrà avere una ragionevole misura del successo dell'adozione dell'AI generativa nelle imprese utilizzatrici, in termini di maggiore efficienza interna e/o di maggiori ricavi connessi con le più elevate caratteristiche dei prodotti e servizi realizzati con il supporto dell'AI generativa.Come è strutturato il *tech stack*? Seguendo lo schema riportato da The Economist in un articolo di quasi un mese e mezzo fa (che riprenderò nel seguito) – *"Just how rich are businesses getting in the AI gold rush? Nvidia and Microsoft are not the only winners"* – esso può essere visto (continua…)
https://www.agendadigitale.eu/mercati-digitali/ia-generativa-rivoluzione-o-bolla-tutti-i-conflitti-che-pesano-sul-futuro/
Agenda Digitale - *Umberto Bertelè - 2 mag 2024*

Hacker Sentenced After Years of Extorting Psychotherapy Patients

Two years after a warrant went out for his arrest, Aleksanteri Kivimäki finally has been found guilty of thousands of counts of aggravated attempted blackmail, among other charges.
Aleksanteri Kivimäki, a Finnish national, has been sentenced to six years and three months in prison, after stealing thousands of patient records from a psychotherapy clinic and using them to blackmail their owners.
A judge in the district court of Länsi-Uusimaa, Finland, sentenced Kivimäki, 26, on April 30 after finding him guilty of 9,231 counts of aggravated dissemination of information infringing on individuals' private lives, and 20,745 counts of aggravated attempted blackmail. He also was found guilty on 20 counts of aggravated blackmail.
Kivimäki, known online as "Zeekill," breached Psychotherapy Center Vastaamo Oy's IT system in November of 2018. It was after this that sensitive information of the clinic's patients started to be posted online. Kivimäki would demand a ransom of €200 ($213) in order not to leak targets' data, upping the payment to €500 ($534) if the ransom wasn't paid in 24 hours.

Kivimäki ultimately caused such a ruckus that Finland's crime figures reportedly rose drastically, to more than double the average rate. (continua…)
https://www.darkreading.com/cyberattacks-data-breaches/hacker-sentenced-after-years-of-extorting-psychotherapy-patients
***Dark Reading** - Dark Reading Staff - May 2, 2024*

GAO: NASA Faces 'Inconsistent' Cybersecurity Across Spacecraft

The space agency needs to implement stricter policies and standards when it comes to its cybersecurity practices, but doing so the wrong way would put machinery at risk, a federal review found.

NASA has gone some way to addressing its cybersecurity challenges, according to a government watchdog, but, it says, too many of its security policies and standards are still optional.

The US Government Accountability Office (GAO) recently completed a review of three NASA projects: the Gateway Power and Propulsion Element, the Orion Multi-Purpose Crew Vehicle, and the Spectro-Photometer for the History of the Universe, Epoch of Reionization and Ices Explorer (SPHEREx). GAO found that contracts relating to these projects required contractors to address cybersecurity by, for example, adequately addressing and testing positioning, navigation, and timing systems.

However, since issuing its Space System Protection Standard in 2019, NASA hasn't updated its policies and standards pertaining to those contracts. Plus, NASA issued a Space Security: Best Practices Guide last December, but the guidance is optional for spacecraft programs.

In concluding its report, GAO recommended that NASA "develop a plan with time frames" to update its policies.

Solving security at NASA is "not going to happen overnight," notes Kevin Kirkwood, deputy CISO at LogRhythm. "It's going to be an interesting and long journey: first to get the foundation in place from a policy perspective, and then the technology has to follow that through. And if they don't figure out a way to make it work, they're going to be in worse trouble than they are today."

Security vs. Practicality

In his response to the report, NASA CIO Jeffrey Seaton agreed with "the need to ensure continuous improvement of policies and standards," but pushed back on GAO's final recommendation. Among his reasons, Seaton pointed out two inescapable realities of cybersecurity in space. (continua…)
https://www.darkreading.com/ics-ot-security/gao-nasa-faces-inconsistent-cybersecurity-across-spacecraft
***Dark Reading** - Nate Nelson- May 3, 2024*

NOTIZIE D'INTERESSE:

Le indicazioni per chi vuole iscriversi come nuovo socio sono contenute nel sito AIIC al link
http://www.infrastrutturecritiche.it/new/per-iscriversi/

Preghiamo i soci che, per vari motivi, modificano la loro anagrafica (recapiti telefonici, indirizzo email o altro) di comunicare I nuovi dati a segreteria@infrastrutturecritiche.it. La mancanza di tali comunicazioni potrebbe impedire, al socio, la ricezione delle comunicazioni.

RIFERIMENTI DELL'ASSOCIAZIONE

AIIC è una associazione apolitica il cui scopo è promuovere attività e conoscenze nell'ambito delle infrastrutture critiche, della loro gestione, protezione e sicurezza.

Per maggiori informazioni sull'Associazione inviare una mail a

segreteria@infrastrutturecritiche.it

o visitate il sito

www.infrastrutturecritiche.it

ATTENZIONE

Per ricevere questa newsletter è necessario inviare una richiesta all'indirizzo
segreteria@infrastrutturecritiche.it

L'iscrizione alla newsletter NON comporta alcun onere e non è richiesta la comunicazione di alcun dato personale ad eccezione dell'indirizzo di posta elettronica.

Sede operativa e servizio di segreteria	AIIC c/o NITEL – via Urbino 31 – 00182 ROMA Tel. +39 06 64871209 E-mail: segreteria@infrastrutturecritiche.it
Gruppo di user all'interno della community	AIIC ha costituito un proprio gruppo di user all'interno della community di LinkedIn: per unirsi al gruppo si può usare il link http://www.linkedin.com/ groups/96335
Versione stampabile della newsletter	Nella sezione "Newsletter"del sito http://www.infrastrutturecritiche.it è disponibile l'archivio delle Newsletter.
Comitato di Redazione	Alberto Traballesi Glauco Bertocchi Silvano Bari Gianluca Cipriani Marco Raul Massoni *ai quali potete inviare suggerimenti e quesiti scrivendo a: segreteria@infrastrutturecritiche.it*

La NewsLetter ha lo scopo di rendere note le principali informazioni nell'ambito delle Infrastrutture Critiche e le attività dell'Associazione Italiana esperti in Infrastrutture Critiche (AIIC). Tutti i contenuti relativi alla sezione NEWS e Eventi sono pubblici on line e di proprietà dei rispettivi editori.